UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/648,149 | 08/25/2003 | William H. Saito | IOSOFTW.003A | 3524 |

20995 7590 02/01/2008
KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

| EXAMINER | |
|---|---|
| LANIER, BENJAMIN E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 02/01/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com
eOAPilot@kmob.com

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/648,149 | **Applicant(s)**<br>SAITO, WILLIAM H. | |
| | **Examiner**<br>Benjamin E. Lanier | **Art Unit**<br>2132 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 December 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 August 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 21 December 2007 has been entered.

### *Response to Amendment*

2. Applicant's amendment filed 21 December 2007 amends claim 1. Applicant's amendment has been fully considered and entered.

### *Response to Arguments*

3. Applicant argues, "the Applicant notes that none of the references disclose the concept of a system that allows access to a secured component having an input by sending a uniquely generated code to a communication device, such as a cell phone, that the user can then use to input into the input in the same format that they would ordinarily input into the input of the at least one secured communication device (*See, e.g.,* Claim 1 as amended.)...with respect to Ueshima, the Applicant notes that Ueshima will be transmitting access information from a cell phone via a radio communications interface (*See,* Ueshima, Column 16, at about line 35)."

4. Examiner notes that the claims do not require, "sending a uniquely generated code...in the same format that they would ordinarily input into the input of the at least one secured communications." The claims merely require that the uniquely generated code be input in a first format and Ueshima discloses that the password can be transmitted to the authentication unit of

the ATM via the radio communications interface (Col. 16, lines 33-35) or the user can manually input the password using a keyboard provided at the ATM (Col. 15, lines 8-14).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 1-3, 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima, U.S. Patent No. 6,731,731, in view of Fernandes, U.S. Publication No. 2003/0218066. Referring to claim 1, Ueshima discloses a method and system for accessing an ATM with a cellular phone instead of using an ATM card (Col. 12, lines 9-15), which meets the limitation of alternative access to the at least one secured component. The system utilizes a register table (Figure 1, 31) that includes the user information for each user who has registered for the authentication service (Col. 12, lines 50-52). The user information includes telephone/cell phone number of the user (Col. 12, lines 53-55 & Col. 16, lines 13-15), user id (Col. 12, lines 56-62), pager number (Col. 13, lines 1-3), and types of service available (Col. 13, lines 10-15), which

meets the limitation of at least one record that includes information about each of the plurality of individuals, the information including a communication path which defines how to contact the individual's communication device and further defines a security protocol for allowing access to the secure component wherein the security protocol further defines whether the individual can access the secured component via an alternative path incorporating the individual's communication device. To authenticate the user at the ATM using their cellular phone, the user makes a call using their cellular phone and requests the generation of a password (Col. 16, lines 11-13). A database searches the register table for the caller's telephone number identified by the caller's number identifying unit (Col. 16, lines 13-15). If a match is found in the database for the user, a password is generated and sent to the user's cellular phone (Col. 16, lines 15-20), which meets the limitation of in response to one of the individuals seeking access to the at least one secure component, retrieving the security protocol and communications path from the at least one record. Ueshima does not disclose that the password can be requested using the ATM interface. It would have been obvious to one of ordinary skill in the art at the time the invention was made to enable the user of Ueshima to request a password using the ATM interface as opposed to making a call using their cellular phone since the system is designed for the user to be proximate to the ATM (Figure 1 & Col. 16, lines 30-39, which details using a radio communication interface to transmit the password from the cellular phone to the ATM) and providing a means for requesting the password using the ATM interface would be more convenient, as a user, than having to physically make a telephone call and vocally request a password or navigate through a series of menus to request a password. This meets the limitations of the controller receiving signals from the input of the at least one secure component in response to the individual manipulating the input device indicating the individual seeks alternative access to the at least one secured device, wherein the controller evaluates the signal received from the input device of the secure component. The ATM and cellular phone each include a radio communication interface for transmitting/receiving password data (Col. 16, lines 5-10 & 33-39), which meets the limitation of a communications interface that allows signals between the communications device carried by the individual and the controller. Ueshima discloses that the generated password is sent to the user's cellular phone through a mail server (Col. 16, lines 15-20), which meets the limitation of sending a first signal to the communications device of the individual via the public communications system in response to the individual seeking access to the at least one secure component wherein the first signal includes a uniquely generated code. Ueshima discloses that the once the user receives the password on their cellular phone, the password can be transmitted to the authentication unit of the ATM via the radio communications interface (Col. 16, lines 33-35) or the user can manually input the password using a keyboard provided at the ATM (Col. 15, lines 8-14), which meets the limitation of a uniquely generated code that is to be input by the individual via the input. Once received by the ATM, the password is authenticated allowing the user to operate a bank account by the ATM (Col. 16, lines 40-45), which meets the limitation of evaluating a response signal via the secured component by the individual by comparing the response signal to the security protocol to determine whether to allow alternative access by the individual to the at least one secure component. Ueshima discloses that that authentication unit of the ATM can include the password table such that the database does not have to be contacted to reference the stored password (Col. 16, lines 56-58) and that the authentication unit has access to the register table with user information (Figure 1), which meets the limitation of a controller having access to the at least one record. However, Ueshima does not specify that the password is transmitted from the authentication unit of the ATM, to the user's cellular phone, once generated. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication unit to include the password generation unit such that the authentication unit transmits the generated password to the user's cellular phone in addition to storing the generated password (Ueshima: Col. 16, lines 56-68) in order to provide complete financial transactions via near-proximity means that results in lower risk assignment by card issuers and resultant lower transaction fees as taught by Fernandes ([0108]).

Referring to claim 2, Ueshima discloses that prior to generation of the password, the user can be prompted for the user's name (Col. 13, lines 50-52), which meets the limitation of the security protocol comprises sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit an access code using the communications device. In response, the user enters the user name in the cellular phone (Col. 13, lines 52-54) and the user name is ultimately compared against the register table to determine whether the entered user name coincides with a registered name (Col. 14, lines 1-4). If the user's name coincide with that registered in the register table, a password is generated and sent to the user's cellular phone (Col. 14, lines 10-18 & Col. 16, lines 17-20), which meets the limitation of which meets the limitation of comparing the access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the access code.

Referring to claim 3, Ueshima discloses that the register table includes password invalidation conditions (Col. 13, lines 6-9) that include a limited number times the password can be used and a limited time period the password can be used (Col. 15, lines 50-65), which meets the limitation of the at least one record further includes additional security criteria and wherein the controller allows access to the at least one secure component only when the individual has satisfied the security protocol and the additional security criteria.

Referring to claim 5, Ueshima that the once the user receives the password on their cellular phone, the password can be transmitted to the authentication unit of the ATM via the radio communications interface (Col. 16, lines 33-35) or the user can manually input the password using a keyboard provided at the ATM (Col. 15, lines 8-14). Once received by the ATM, the password is authenticated allowing the user to operate a bank account by the ATM (Col. 16, lines 40-45), which meets the limitation of evaluating whether the individual correctly entered the access code on the input of the at least one secure component. Ueshima discloses that that authentication unit of the ATM can include the password table such that the database does not have to be contacted to reference the stored password (Col. 16, lines 56-58) and that the authentication unit has access to the register table with user information (Figure 1), which meets the limitation of a controller having access to the at least one record. However, Ueshima does not specify that the password is transmitted from the authentication unit of the ATM, to the user's cellular phone over the radio communications interface, once generated. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the authentication unit to include the password generation unit such that the authentication unit transmits the generated password to the user's cellular phone over the radio communications interface, in addition to storing the generated password (Ueshima: Col. 16, lines 56-68) in order to provide complete financial transactions via near-proximity means that results in lower risk assignment by card issuers and resultant lower transaction fees as taught by Fernandes ([0108]).

Referring to claim 6, Ueshima discloses that prior to generation of the password, the user can be prompted for the user's name (Col. 13, lines 50-52), which meets the limitation of sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit a first access code using the communications device. In response, the user enters the user name in the cellular phone (Col. 13, lines 52-54) and the user name is ultimately compared against the register table to determine whether the entered user name coincides with a registered name (Col. 14, lines 1-4), which meets the limitation of comparing the first access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the first access code. If the user's name coincide with that registered in the register table, a password is generated and sent to the user's cellular phone (Col. 14, lines 10-18 & Col. 16, lines 17-20), which meets the limitation of sending a second access code to the communications device in response to determining that the individual correctly entered and transmitted the first access code. Ueshima that the once the user receives the password on their cellular phone, the password can be transmitted to the authentication unit of the ATM via the radio communications interface (Col. 16, lines 33-35) or the user can manually input the password using a keyboard provided at the ATM (Col. 15, lines 8-14). Once received by the ATM, the password is authenticated allowing the user to operate a bank account by the ATM (Col. 16, lines 40-45), which meets the limitation of evaluating whether the individual successfully entered the second access code on the input of the secure component before allowing access to the secure component.

Referring to claim 7, Ueshima discloses that the cellular phone includes means allowing communication over a cellular phone network (Figure 1, 110) between the cellular phone (Figure 1, 111) and the ATM (Figure 1, 60), which meets the limitation of the communications interface comprises a modem that is adapted to provide cellular telephone communication between the controller and cellular telephone devices carried by the plurality of individuals.

Referring to claims 8, 9, Ueshima discloses that prior to generation of the password, the user can be prompted for the user's name (Col. 13, lines 50-52). In response, the user enters the user name in the cellular phone (Col. 13, lines 52-54) and the user name is ultimately compared against the register table to determine whether the entered user name coincides with a registered name (Col. 14, lines 1-4). If the user's name coincide with that registered in the register table, a password is generated and sent to the user's cellular phone (Col. 14, lines 10-18 & Col. 16, lines 17-20), which meets the limitation of the at least one record further includes supplemental commands and corresponding actions wherein the controller, in response to the receiving a supplemental command from a user, induces the system to implement the corresponding action, the supplemental command comprises an additional access code provided to the controller via the communications interface by the individual communications device.

Referring to claim 10, Ueshima discloses that if the entered user name does not coincide with registration information in the register table, an error message is displayed and not password is generated (Col. 14, lines 4-9), which prevents access to the ATM, which meets the limitation of the supplemental command induces the controller to limit access to the at least one secure component.

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima, U.S. Patent No. 6,731,731, in view of Fernandes, U.S. Publication No. 2003/0218066 as applied to claims 1-3 above, and further in view of Nobrega, U.S. Publication No. 2002/0107791. Referring to claim 4, Ueshima discloses that the cellular phone transmits the password to the ATM via the radio communication interface (Col. 16, lines 33-35), but does not specify that the cellular phone location information be transmitted along with the password to the ATM. It would have been obvious to one of ordinary skill in the art at the time the invention was made in order to verify that the cellular phone is in the same geographic region as the ATM as taught by Nobrega ([0066]). This type of verification would serve to ensure that any access given to the ATM would be given to the appropriate person proximate to the ATM.

9. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueshima, U.S. Patent No. 6,731,731, in view of Fernandes, U.S. Publication No. 2003/0218066 as applied to claim 1 above, and further in view of Fung, U.S. Patent No. 6,859,882. Referring to claims 11-12, Ueshima does not disclose the authentication system remotely enabling the ATM by sending a wake-on-LAN signal to the ATM. Fung discloses an e-commerce system where sites are remotely enabled using wake on LAN signal events (Col. 69, line 53 – Col. 70, line 4), which meets the limitation of the controller is adapted to remotely enable the secure component when the controller receives an enablement signal from the individual via the communications interface, the controller remotely enables the secure component by sending a wake on LAN signal to the at least one secure component. It would have been obvious to one of ordinary skill

in the art at the time the invention was made for the ATMs of Ueshima to be remotely enabled using wake on LAN signal events in order to conserve power based on the varying demand that may be placed on the ATMs as taught in Fung (Col. 34, lines 7-39).

## *Conclusion*

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier
Primary Examiner